

## Şehit Albay İbrahim Karaođlanođlu İmam Hatip İin Sunulan Eylem Planı - 21.09.2021 @ 12:50:58

### Altyapı Teknik gvenlik

- › Her yařtan ğrencide eđitimsel bir yaklařım ve dayanıklılık oluřturmak da gvenli ve sorumlu evrimii kullanımın anahtarıdır, bu nedenle tm đretmenleri đrencileriyle iyi ve gvenli bir dijital vatandař olma konusunda nasıl konuřacakları hakkında bir tartiřma yapmak iin bir araya getirin Rol yapma ve grup oyunları aracılıđıyla bu konuda sınıfta gerekleřebilecek tartiřma rnekleri iin [www.europa.eu/youth/EU\\_en](http://www.europa.eu/youth/EU_en) bakın.
- › Bİt hizmetlerinizin artık kullanılmazsa dzenli olarak gzden geirilmesi, gncellenmesi ve kaldırılması iyi bir uygulamadır.

### đrenci ve personelin teknolojiye eriřimi Veri koruması

- › đrenci verilerini řifrelemek ve gvenli bir řekilde depolamak iin iyi bir politikanız vardır. Tm yeni personelin řifreleme ve veri iřleme prosedrlerinden haberdar olduđundan ve okulunuz iin veri denetleyicisi olarak hareket eden adlandırılmıř bir iletiřim noktası olduđundan emin olun. Diđer okulların deneyiminizden yararlanabilmesi iin bir řifreleme sistemi aracılıđıyla hassas verileri korumayla ilgili bazı ynergeleri okul profilinize ykleyin.
- › đrenme ve ynetim ortamlarınızı ayrı tutmak iin iyi bir politikanız vardır. Politikalarınızı gzden geirmeye devam ederken, bu ortamları ynetme konusunda personel eđitiminin gncel olduđundan emin olmak iyidir. Politikanızı okul profilinize ykleyerek diđer eGvenlik Etiketi kullanıcılarıyla paylařın.
- › Okulunuzun cihazları, zellikle tařınabilir cihazları korumanın nemine dair materyaller sađlaması iyidir. Personelin bunlardan haberdar olduđundan ve kullandıđından emin olun. Bu malzeme, indksiyonlarının bir parası olarak yeni personele iřaret edilmelidir. Ltfen bunları kanıt olarak yklemeyi ve forumda bařkalarıyla paylařmayı dřnn. Ayrıca, malzemelerinizin en son teknolojinin durumuna uygun olduđundan emin olmak iin dzenli olarak gzden geirildiklerinden emin olun.

## Yazılım lisansı

- › Sorumlu personelin yüklü yazılımların ve lisans durumlarının tamamen farkında olması iyi bir uygulamadır.
- › Lisans sözleşmelerine uygunluk önemlidir. Bunun gerçekleştiği ve tüm lisansların amaç için geçerli olduğundan emin olmak için birinin genel sorumluluğa sahip olması gerekir. Vikipedi'deki Son [kullanıcı lisans sözleşmesi bölümü hüküm](#) ve koşulları anlamak ve yazılım sözleşmelerini karşılaştırmak için yararlı bilgiler sağlayacaktır.
- › Okulunuzdaki tüm yazılımların yasal olarak lisanslandığından ve lisansların kopyalarının merkezi olarak tutulduğundan emin olmanız gerekir. Ayrıca, BT sistemlerinizi destekleyen kişiye yazılımın sistem güvenliğinden ödün vermeyeceğini kontrol etmeniz gerekir. Okulunuz yazılım edinimi için net bir politika geliştirmelidir ve bu süreci mümkün olan her yerde merkezileştirmek iyi bir uygulamadır.

## BT Yönetimi

- › Okulunuzda yalnızca baş usta ve/veya BT sorumlusu yeni yazılım edinebilir. Öğretmenlerin bürokratik olmayan ve zamanında yeni yazılım isteyebilecekleri bir sistem koymayı düşünün. Bu, öğretmenlerin yetkisiz kopyalamanın cazibesi ve doğasındaki tehlikeler ve maliyetler olmadan daha ilgi çekici bir ders oluşturmalarını sağlar.
- › Okul bilgisayarlarında yüklü olan yeni yazılımların kullanımında rehberlik sağlamak ve/veya eğitmek iyi bir uygulamadır. Bu, okul üyelerinin yeni özelliklerden yararlanmasını, aynı zamanda ilgili durumlarda güvenlik ve veri koruma sorunlarının farkında olmalarını sağlar.

## Politika

### Kabul Edilebilir Kullanım İlkesi (AUP)

- › eGüvenlik'in çeşitli okul politikalarının ayrılmaz bir parçası olması mükemmeldir. Tüm personel öğretimleri aracılığıyla uygun olduğunda buna atıfta bulunmuyor mu? İyi uygulama örnekleri arayın ve bunları personel ve öğrencilerle paylaşın. Bu iyi uygulamayı vurgulamak ve diğerlerine ilham kaynağı olarak [Okulum alanınız](#) üzerinden eSafety Label portalındaki profilinize yüklemek için kısa bir vaka çalışması üretin okullara.

- › Okulunuzda okul politikalarının her yıl gözden geçirilmesi iyidir. Bunları etkileyebilecek değişiklikler yapıldığında bunların da güncelleştirildiğinden emin olun. Tüm personel poliçenin içeriğinden haberdar olmalıdır.

## Raporlama ve Olay İşleme

- › Yeni personel üyeleri de dahil olmak üzere tüm personelin, bir okul makinesinde uygunsuz veya yasadışı materyal bulunması durumunda ne yapılması gerektiğinin farkında olduğundan emin olun. İlkenin titizlikle uygulandığından da emin olun. Okulun üst düzey liderlik ekibinden biri bunu izlemeli.

## Personel politikası

- › Okulunuzda kullanıcı hesapları zamanında yönetilir. Bu, yanlış kullanım riskini azaltıklarından önemlidir.
- › Okul politikasının akıllı telefonlar gibi potansiyel olarak güvenli olmayan cihazlarla ilgili riskler hakkında bilgi içermesi ve bu referansın yapılması iyi bir uygulamadır. Okul politikanızı, Okulum alanından da erişilebilen yükleme kanıtı aracı aracılığıyla paylaşmayı düşünün.

## Öğrenci pratiği/davranışı

- › Müfredat, öğrencilerin okul aktivitelerini günlük yaşamlarında olup bitenlerle şekillendirmeleri için çok sıkıdır. Bu, öğrenciler daha meşgul olacağı ve öğretmenin gerçek yaşam sorunlarını tanınmasına izin verdiği için ithal değildir. Çevrilmiş bir sınıfın muhtemel yetlerini keşfedin ve/veya ödevlerinin bir parçası olarak medya kullanımları ve sorunları hakkında bilgi paylaşmalarına izin verin.
- › Kabul Edilebilir Kullanım Politikanızda elektronik iletişim yönergeleri tanımladınız ve bu diğer okullar için yararlı bir iyi uygulama örneği olacaktır. Öğrenciler için \_ elektronik iletişim yönergeleri hakkında bir öğretici oluşturabilir ve okulum aracılığıyla okul profiline yükleyebilir misiniz, \_ böylece diğer okullar deneyiminizden faydalanabilirsiniz.
- › Okulunuz, öğrenci davranışı için olumlu ve olumsuz sonuçlar konusunda okul çapında bir yaklaşıma sahiptir. Bu iyi bir uygulamadır, lütfen politikanızı eSafety portalının Okulum alanı aracılığıyla paylaşın, böylece diğer okullar bundan ders alabilir.

## Çevrimiçi okul varlığı

- › Okulda fotoğraf ve video çekme ve yayınlama hakkındaki bilgi formuna bakın ([www.esafetylevel.eu/group/community/taking-and-publishing-photos-and-videos-at-school](http://www.esafetylevel.eu/group/community/taking-and-publishing-photos-and-videos-at-school)) to see that your Okul Politikası tüm alanları kapsar, ardından Okul Politikanızın bu bölümünü My okul alanınız üzerinden profil sayfanıza yükleyin böylece diğer okullar sizin iyi uygulamanızdan öğrenebilir.
- › Öğrencilerin okulun çevrimiçi varlığı hakkında geri bildirimde bulunabilmesi iyidir. Tamamen öğrenciler tarafından yönetilen bir alan yaratmayı düşünün. Medya okuryazarlığı ve ilgili konular hakkında bilgi edinmek için harika bir fırsat. Ayrıca bir eş destek ağı kurulmasına yardımcı olabilir. eSafety Label bilgi sayfasında daha fazla bilgi edinin.

## Egzersiz

### Müfredatta eGüvenlik eGüvenliğinin Yönetimi

- › Bu konuların eGüvenlik müfredatında yer almış olması iyidir. Yeni ve ortaya çıkan konuların ele alınması için eGüvenlik eğitiminizin kapsadığı konuları düzenli olarak gözden geçirmek iyi bir fikirdir.
- › Çevrimiçi eylemlerin sonuçlarının tüm sınıflardaki öğrencilerle tartışılması mükemmeldir. Sözleşme koşullarını tam olarak anlamak için hüküm ve koşulların okunması gerekir. Bu, veri gizliliğinin yönleriyle de ilgilenebilir. Bir diğer önemli konu da telif hakkı ihlalidir. Lütfen yüklemeye kanıt aracı aracılığıyla kullanılan materyalleri paylaşın, Okul alanım aracılığıyla da erişilebilir.
- › Okulunuzda Siber Zorbalık'ın müfredatta küçük yaştan itibaren öğrencilerle tartışılması iyi bir uygulamadır.
- › Okulunuzda, öğrencilere küçük yaşlardan itibaren sosyal medyayı kullanırken sorumluluklar ve sonuçlar hakkında öğretilmesi çok iyidir. Lütfen okul alanım üzerinden de erişilebilen yüklemeye kanıt aracı aracılığıyla kaynakları paylaşın.

## Müfredat dışı aktiviteler

- › Ulusal Safer İnternet'inizdeki çevrimiçi eGüvenlik kaynaklarını sık sık kullandığınızı bilmek iyidir. Orta. Bu kaynakları okulunuzda yararlı buldunuz mu? Lütfen \_ kullanımları ve değerleri hakkında geri bildiriminizi [info-insafe@eun.org](mailto:info-insafe@eun.org) gönderin.
- › Öğrencilerinizin çevrimiçi alışkanlıkları hakkında sahip olduğunuz bilgileri eSafety Label topluluğu aracılığıyla diğer okullarla paylaşmayı düşünün. Örneğin, öğrencilerin çevrimiçi \_ alışkanlıklarıyla ilgili en son anket bulgularınızı Okul \_ [Alanım](#) [alanınız](#) aracılığıyla okul profilinize yükleyebilirsiniz.
- › Öğrencilerin akran mentorluğuna olan etkileşimlerini daha da geliştirmeye çalışın ve onlara düşüncelerini ve anlayışlarını akranlarıyla paylaşmaları için daha fazla fırsat sağlayın. Ayrıca daha fazla fikir ve kaynak elde etmek için eSafety Label portalının kaynak bölümüne göz atın.

## Destek kaynakları

- › EGüvenlik konularında öğrencilere güven öğretmeni olarak hareket eden bir personele sahip olmak harika.
- › Gençler akranlarının tavsiyelerine daha açık. EGüvenlik konularında veya öğrencilerde uzman bilgilerini teşvik eden ve daha sonra akranları için bir referans noktası haline gelebilecek isteğe bağlı kurslar ve/veya okul ödülleri sunmayı düşünün.

## Personel eğitimi

- › Öğretmenlere öğrencilerin boş zamanlarında kullandıkları teknoloji hakkında bilgi vermeniz iyi bir uygulamadır. Bu farkındalık, okul için elektrik kesintisi sorununu ele almanın ilk adımı olduğu için önemlidir. Aynı zamanda öğrencilerden ödevlerini okul dışında bulunmayan teknolojiyi kullanarak yapmaları istenmemelidir. \_ [Okullarda BİT'in Essie Anketine](#) \_ bir göz atmak isteyebilirsiniz.